AMENDMENTS TO THE CLAIMS:

Please amend the claims as follows. This listing of claims will replace all prior versions and listings of claims in the application.

1.-18. (Cancelled)

19. (Previously Presented) A random number generator, comprising:

a true random number generator;

a pseudo-random number generator arranged to generate a pseudo-random sequence by using the true random numbers produced by said true random number generator as random seed; and

a mixing logic connected between said true random number generator and said pseudo-random number generator and arranged to alter the behavior of said pseudo-random number generator by using the random seed,

said true random generator being arranged to generate a random sequence of bits having variable rate, and said mixing logic comprising a generator of an alteration signal intended to change the behavior of said pseudo-random number generator at multiple random instants in the interval between two subsequent seeds, thereby obtaining in said interval multiple pseudo-random sequences of random lengths shorter than the random length determined by the arrival of two subsequent seeds, said generator of the alteration signal being connected so as to receive said seed and generate said alteration signal by processing said seed by means of the sequence generated by said pseudo-random number generator.

20. (Previously Presented) The random number generator as claimed in claim 19, wherein said generator of the alteration signal comprises:

a first down counter arranged to count down from a first random number represented by a first group of bits which are part of a randomly rotated version of a seed received by said alteration signal generator, said first counter loading said first random number and starting its countdown whenever a seed is available and, between the occurrence of two subsequent seeds, whenever it generates a terminal count signal, said terminal count signal being fed to said pseudo-random number generator as alteration signal;

a second down counter which is arranged to count down from a second random number represented by a group of bits of the sequence generated by said pseudo-random number generator and is arranged to load a new value of said second random number and to start again its countdown whenever said first down counter generates its terminal count signal; and

a recirculating shift register which receives the seeds and feeds said first down counter with said first random number, and which is arranged to generate said randomly rotated version of the seed in the intervals between the arrivals of two subsequent seeds by rotating the bits of the seed by an amount determined by the value of said second random number.

21. (Previously Presented) The random number generator as claimed in claim 19, wherein said pseudo-random generator is a linear feedback shift register and said alteration signal generator supplies said alteration signal to the feedback logic of said linear feedback shift register.

22. (Previously Presented) The random number generator as claimed in claim 19, wherein said mixing logic further comprises an input circuitry arranged to receive the random sequence of bits generated by said true random generator to build

said seed by parallelising the bits of said random sequence and to generate a signal indicating the availability of a seed.

23. (Previously Presented) The random number generator as claimed in claim 20, wherein said recirculating shift register is arranged to load a seed directly whenever it receives said signal indicating the availability of the seed, and said pseudo-random generator is arranged to load a new seed upon command of said first counter whenever the latter receives said signal indicating the availability of the seed.

24. (Previously Presented) The random number generator as claimed in claim 19, wherein said input circuitry comprises a clock signal generator for generating, starting from a first clock signal timing the operations of said input circuitry, and a second clock signal for timing said pseudo-random generator and said alteration signal generator whereby the output bit rate of the random number generator is independent of the rate of the random sequence of bits supplied by the true random generator.

25. (Previously Presented) The random number generator as claimed in claim 19, further comprising an output logic for parallelising the altered pseudo-random sequence and building words of a given length, said output logic comprising a scrambler for scrambling the bits in each word in random manner.

26. (Previously Presented) The random number generator as claimed in claim 25, wherein said scrambler is controlled by a random selection signal provided by said generator of the alteration signal.

27. (Previously Presented) The random number generator as claimed in claim 20, wherein a random selection signal is supplied by said recirculating shift register.

28. (Previously Presented) The random number generator as claimed in claim 25, wherein said scrambler circuit comprises a switching matrix comprised of an n-level binary tree of switches, each controlled by a respective bit of said random selection signal so as to scramble or to let through unchanged its input bits.

29. (Previously Presented) The random number generator as claimed in claim 25 implemented as an integrated circuit.

30. (Previously Presented) A method of generation of random numbers, in which said random numbers are generated by altering a pseudo-random sequence by means of true random numbers forming random seeds for the generation of said pseudo-random sequence, the method comprising the steps of:

obtaining the random seeds from a random sequence of bits having variable rate;

processing a random seed to generate an alteration signal exploiting the random arrival time of the bits of said sequence of bits; and

changing the pseudo-random sequence by said alteration signal at random instants between the arrival of two subsequent seeds, thereby obtaining in said interval multiple pseudo-random sequences of random lengths shorter than the lengths determined by the arrival of two subsequent seeds, said alteration signal being generated under the control of the pseudo-random sequence.

31. (Previously Presented) The method as claimed in claim 30, wherein said alteration signal is generated at the end of a first countdown starting from a first random number represented by a randomly variable group of bits that are part of a rotated version of a received seed obtained by rotating the seed by an amount indicated by a

second random number represented by a group of bits of the pseudo-random sequence, the first countdown starting whenever a seed is generated and restarting, between the arrival of two subsequent bits, whenever the countdown itself ends; and wherein said second random number is the starting value of a second countdown starting whenever the first down counting ends, the end of said second countdown stopping said seed rotation.

32. (Previously Presented) The method as claimed in claim 30, wherein said pseudo-random sequence is generated by a linear feedback shift register and said alteration signal is fed to the feedback logic of said linear feedback shift register.

33. (Previously Presented) The method as claimed in claim 30, wherein the altered pseudo-random sequence is parallelised to create words of a desired length and further comprising a random scrambling of said words.

34. (Previously Presented) The method as claimed in claim 33, wherein said scrambling is controlled by a random selection signal obtained from the bits used to form said first random number.

35. (Previously Presented) A method as claimed in claim 30, further comprising the step of generating, starting from a first clock signal timing the seed generation and a second clock signal for timing the generation of said pseudo-random sequence and of said alteration signal, the parallelisation of the output words and the scrambling, whereby an output bit rate independent from the rate of the random sequence of bits is obtained.

36. (Currently Amended) A computer readable medium encoded with a computer program product loadable ~~in the~~ into a memory of at least one computer and including software code portions capable of performing the method of claim 30.